vortex™

Helping banks reach out

Secure your ATM fleet with

Vortex Terminal Security

PA-DSS VALIDATED

www.vortexindia.co.in

Self-service terminals with its inherent hardware and software architecture are vulnerable to both physical and cyber attacks unless sufficient protection mechanisms are put in place. From resorting to methods such as skimming and USB sticks or CDs to install malware within Automated Teller Machines (ATMs) to connect to and control peripheral devices to withdraw stored cash and/or collect card/account information of customers which require physical presence, the attacks have now gotten into the bank's data center networks, making it even harder to detect. Cyber criminals are now resorting to means that enable them to access and control ATMs through bank networks. Vortex Terminal Security offerings feature a comprehensive set of security solutions to keep your Vortex ATMs more secure and safe.

Intrusion Protection

Logical attacks and data attacks are high impact threats on unattended terminals when compared to visible or physical breaches. ATMs are vulnerable to malwares, viruses, hacking and other deceptive attacks. Self-service terminals are soft targets to carry out such attacks leading to identity thefts and transactional frauds. Intrusion Protection systems safeguard terminals from malwares, viruses and all emerging threats including zero-day attacks. In Vortex ATMs, whitelisting of applications, services and processes is done through AppArmor. AppArmor is a Linux kernel security module that restricts application capabilities with specific profiles. Profiles can allow or disallow capabilities like network access, raw socket access, peripheral communication port access and system permissions to read, write or execute. AppArmor supplements Unix Discretionary Access Control (DAC) model by providing Mandatory Access Control (MAC).

1. Network Integrity

Firewall and network parameter control and configuration is established through inbound and outbound rule sets authorizing hosts, protocols and networks. Network communication protocol encryption with TLS sockets protects sensitive transaction messages between terminal and hosts. In addition, MAC is also supported in the protocol to ensure message integrity and tamper detection.

2. USB Whitelisting

USB Whitelisting disallows any mounting of disk drives outside of Swave application's control. Mounting of USB drives via terminal prompts is not allowed. Hence usage of USB drives by unauthorized person in ATM is made impossible. Any unauthorized usage of USB ports to mount storage drives or other devices is prevented.

3. System Integrity

System integrity rules block application execution if integrity fails.

4. Whitelisting – AppArmor★

Protects the terminal from unauthorized applications and executables. Rule sets authorizing the terminal application binaries and essential software components ensures protection from rogue applications taking control. Only the authorized terminal application has access to peripheral devices and ports in the terminal. No other application can gain access to hardware devices and ports.

5. Hard Disk Encryption★

Hard Disk Encryption will protect against ATM cores or hard disks being stolen and used to reverse engineer ATM software or harvest data on the hard disk. Encryption allows ATM to have encrypted file system and at the same time be capable of unattended booting.

Note: ★ marked are optional items – part of advanced security features

Access Protection

While addressing ATM security threats, focusing only on external threats will be of major deficiency. Organisations must secure access to their systems to prevent data misuse and unauthorized access and ensure smooth function of the end point terminals. Access Protection delivers authorized use of software environment and shuts down the ATM from abuse.

1. OS Hardening

It prunes the role of the terminal operating system to the minimum required mode, allowing only the required functions and services. Vortex ATMs are installed with a hardened operating system - a trimmed version of Debian Linux operating system, with only necessary services and software packages required for ATM functionality. Due to this trimming, a great number of application layer related vulnerabilities are averted.

2. Time Based Admin Access ★

Offers one time privileges and time bound secure access privileges for terminal maintenance or upgrade functions.

3. Role and Rights Management of Users

Effective access control sets rights and roles for various user profiles based on non-root user for Swave application and non-root user for Engineer access. Root accounts are disabled with password policies put in place for Swave supervisor users. OS logins using passwords are disallowed with One Time Password based sessions used for secure functions, disabling key combination and terminal access control.

Data Protection

The data protection strategies set by PCI DSS (Payment Card Industry Data Security Standard) for adherence are that the data integrity and confidentiality needs to be preserved while data is in use and in motion. Following are the security measures employed to ensure integrity and confidentiality of data.

1. Access to data in use only by authorization

Application binaries, Security configuration and Security keys are protected through access restrictions. Critical configuration changes are access restricted using OTP mechanism. Application binaries and keys are protected through OS level privilege settings. PA-DSS compliance ensures card holder data is also handled in a secure environment.

2. Encryption of data in move within secure environment

Application binaries installed or upgraded on Vortex ATMs are signed applications which get validated for signatures before installation. Bad signatures result in rejection. The software development and rollout practices are compliant with PA-DSS guidelines, hence ensuring a periodic review of security breaches and preventive measures.

3. Secure communication mechanism between ATM core & Dispenser - Dispenser Host Pairing ★

Avoid 'Black box' attacks on the dispenser using Vortex's host pairing mechanism between the ATM core and Dispenser hardware. Also avoid reverse engineering of dispenser communication.

4. Secure communication protocol between ATM and host

Avoid network based attacks between ATM and host. Enable secure TLS communication protocol between ATM and host to protect card holder data and transaction messages that flow through the network. Enable firewall rules to lock down communication ports so that no rogue channels of communication is established.

Note: ★ marked are optional items – part of advanced security features

Software Management

1. Terminal Application/Patch Update Process

Swave terminal software/patch can be upgraded onsite or remotely through authorized sessions. The software upgrade process requires elevated authorization through an OTP session. During the Swave application boot, the application binary signature is verified and upon successful verification it is allowed to run. The application execution is stopped in case of an invalid signature.

2. Vulnerability Assessment Test

Vortex carries out vulnerability assessments using OWASP Top 10 and SANS CWE Top 25 on a quarterly basis or when significant upgrades are released. Any vulnerability discovered shall be fixed and patches for the same would be rolled out. Authenticated vulnerability assessment test is carried out with the help of OpenVAS and Nessus tool.

3. Security Patch and Update Cycle

Vortex has subscribed to Debian security updates. The updates received are reviewed for ATM upgrading which are done quarterly. High impact security patch updates are done within 24 hours of the OS distribution releases. It can be updated remotely through Perfo® - a Centralized ATM Management Solution.

Physical Protection

ATMs are vulnerable not just for the currency but also for the data they hold, now that user data is more attractive than money! In the past, ATM hardware was manipulated or vandalised to gain access to money in the safety container. But in recent times, the ATM devices have been physically manipulated to capture valuable user credentials. The prevailing physical threats include: Cash trapping, Card trapping, Card Skimming and Breaking-in.

The protection strategies against these attacks involve detection of vandalism or manipulation, leading to alarm trigger and shutdown of system from usage.

1. Thermal/Vibration/Tilt sensors on the safe to detect vandalism and trigger alarms
2. Anti-skimming devices (ASD) fit to card reader to detect skimmer and trigger alarm or shutdown. User's card information is protected from skimming activities with Vortex ASD (which is integrated with card reader). ASD is always active and detects any foreign body which is afifxed to the card reader bezel. Once detected, ASD will close the card reader shutter and render the ATM out of service. Anti-skimming functionalities cannot be disabled in ATMs.

Why Vortex?

Vortex Engineering Private Limited is an innovative and leading provider of Automated Teller Machines (ATMs) and associated services for banks. With the mission of helping banks reach out and having pioneered ATMs for deployment even in the most difficult and challenging environments, Vortex offers a suite of services for ATM management. With a strong foundation built on years of R&D, a steady focus on self-service banking products for emerging markets, Vortex is now changing the face of banking with its new rugged and reliable range of ATMs. Vortex ATMs are designed, developed and manufactured in India. Operating out of its manufacturing facilities in Chennai, Vortex's ISO-certified manufacturing facilities enable the company to bring out a range of top-notch products such as Ecoteller® Mini, Front Load & Rear Load ATM. Ably complementing this infrastructure are its service centres that deliver support with the most comprehensive tools for predictive maintenance. Vortex ATMs are now deployed deployed in several countries in Asia and Africa having 5000+ installations globally.

Connect with us
Email: marketing@vortexindia.co.in

vortex™
Helping banks reach out

No 6B, 6th Floor, IIT Madras Research Park, No.1. Kanagam Road, Taramani
Chennai 600 113, Tamil Nadu, India. Phone: +91 44 66 33 9700
www.vortexindia.co.in